

GeekBrains

Урок 2 Видео 2

Криптография

PKCS#7 padding

В этом видео

1. Что такое паддинг?
2. Назначение паддинга
3. Устройство PKCS#7 паддинга

Длины открытых текстов чаще всего не кратны длине блока шифра.

Например, сообщение “YELLOW” имеет длину 6 байт, в то время как длина блока AES — 16 байт.



PKCS#7 padding

59454c4c4f57205355424d41524902 02

59454c4c04040404

59454c4c4f570a0a0a0a0a0a0a0a0a0a

Паддинг или часть сообщения?

59454c4c4f57205355424d4152492201

55424d415249220
1
1010101010101010
0
1010101010101010
0

59454c4c4f572053
55424d415249220
1

GeekBrains

Итоги

1. Узнали что такое паддинг и зачем он нужен
2. Разобрались как устроен PKCS#7 паддинг